

I. REAL PARTY IN INTEREST

As evidenced by the assignment recorded at Reel/Frame 012531/0808, the subject application is owned by Sun Microsystems, Inc., a corporation organized and existing under and by virtue of the laws of the State of Delaware, and now having its principal place of business at 4150 Network Circle, Santa Clara, CA 95054.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences known to Appellants, Appellants' legal representatives, or assignee which will directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1 – 31 are pending. Claims 1 – 31 are rejected, and the rejection of these claims is being appealed. A copy of claims 1 – 31 is included in the Claims Appendix attached hereto.

IV. STATUS OF AMENDMENTS

Amendments to claims 20 – 23, having been submitted subsequent to the final rejection in an Amendment dated April 17, 2006, have been entered. No other amendments to the claims have been submitted subsequent to the final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a processing unit (see, e.g., FIG. 3, reference numerals 22 and 22'; page 11, line 5 – page 12, line 26) connectable to a data communications network (see, e.g., FIG. 1, reference numerals 2 and 3; page 10, lines 3 – 22). The processing unit has a device reader (see, e.g., FIG. 4, reference numeral 40; page 13, lines 4 – 26) for a portable storage device (see, e.g., FIGs. 4 and 17, reference numeral 54; page 13, line 28 – page 14, line 16). The portable storage device includes storage (see, e.g., FIG. 4, reference numeral 58; page 13, lines 28 – 30; page 20, line 28 – page 21, line 5) operable to supply a network identity (see, e.g., page 11, lines 12 – 29) for the processing unit. The portable storage device also includes an access controller (see, e.g., FIG. 4, reference numeral 59; FIG. 9, reference numeral 160; page 13, line 30 – page 14, line 2; page 20, lines 22 – 23). The access controller is operable to prevent unauthorised writing to the storage (see, e.g., FIG. 9, reference numeral 160; page 20, lines 22 – 23; page 21, lines 7 – 14). The processing unit is operable, before reading the network identity from the portable storage device, to attempt a write to the storage of the portable storage device (see, e.g., FIG. 10, reference numeral 180; page 22, lines 18 – 27). On determining that the write has failed (see, e.g., FIG. 10, reference numerals 184 and 186; page 23, lines 4 – 10), the processing unit is operable to read the supplied network identity (see, e.g., FIG. 10, reference numeral 84; page 14, lines 18 – 28; page 23, lines 8 – 10).

Independent claim 10 is directed to a control program (page 35, lines 23 – 29) for controlling the selection of a network identity for a processing unit (see, e.g., FIG. 3, reference numerals 22 and 22'; page 11, line 5 – page 12, line 26) connectable to a data communications network (see, e.g., FIG. 1, reference numerals 2 and 3; page 10, lines 3 – 22). The processing unit has a device reader (see, e.g., FIG. 4, reference numeral 40; page 13, lines 4 – 26) for a portable storage device (see, e.g., FIGs. 4 and 17, reference numeral 54; page 13, line 28 – page 14, line 16). The portable storage device includes storage (see, e.g., FIG. 4, reference numeral 58; page 13, lines 28 – 30; page 20, line 28 – page 21, line 5) operable to supply a network identity (see, e.g., page 11, lines 12 – 29)

for the processing unit. The portable storage device also includes an access controller (see, e.g., FIG. 4, reference numeral 59; FIG. 9, reference numeral 160; page 13, line 30 – page 14, line 2; page 20, lines 22 – 23). The access controller is operable to prevent unauthorised writing to the storage (see, e.g., FIG. 9, reference numeral 160; page 20, lines 22 – 23; page 21, lines 7 – 14). The control program is operable, before reading the network identity from the portable storage device, to attempt a write to the storage of the portable storage device (see, e.g., FIG. 10, reference numeral 180; page 22, lines 18 – 27). Only on determining that the write has failed (see, e.g., FIG. 10, reference numerals 184 and 186; page 23, lines 4 – 10), the control program is operable to read the supplied network identity (see, e.g., FIG. 10, reference numeral 84; page 14, lines 18 – 28; page 23, lines 8 – 10).

Independent claim 20 is directed to a method of controlling the selection of a network identity for a processing unit (see, e.g., FIG. 3, reference numerals 22 and 22'; page 11, line 5 – page 12, line 26) connectable to a data communications network (see, e.g., FIG. 1, reference numerals 2 and 3; page 10, lines 3 – 22). The processing unit comprises a device reader (see, e.g., FIG. 4, reference numeral 40; page 13, lines 4 – 26) for a portable storage device (see, e.g., FIGs. 4 and 17, reference numeral 54; page 13, line 28 – page 14, line 16). The portable storage device includes storage (see, e.g., FIG. 4, reference numeral 58; page 13, lines 28 – 30; page 20, line 28 – page 21, line 5) operable to supply a network identity (see, e.g., page 11, lines 12 – 29) for the processing unit. The portable storage device also includes an access controller (see, e.g., FIG. 4, reference numeral 59; FIG. 9, reference numeral 160; page 13, line 30 – page 14, line 2; page 20, lines 22 – 23). The access controller is operable to prevent unauthorised writing to the storage (see, e.g., FIG. 9, reference numeral 160; page 20, lines 22 – 23; page 21, lines 7 – 14). The method comprises attempting a write to the storage of the portable storage device (see, e.g., FIG. 10, reference numeral 180; page 22, lines 18 – 27). The method further comprises, only on determining that the write has failed (see, e.g., FIG. 10, reference numerals 184 and 186; page 23, lines 4 – 10), reading the supplied network identity from the portable storage device (see, e.g., FIG. 10, reference numeral 84; page 14, lines 18 – 28; page 23, lines 8 – 10).

Independent claim 25 is directed to a portable storage device (see, e.g., FIGs. 4 and 17, reference numeral 54; page 13, line 28 – page 14, line 16) that includes storage (see, e.g., FIG. 4, reference numeral 58; page 13, lines 28 – 30; page 20, line 28 – page 21, line 5) containing a network identity (see, e.g., page 11, lines 12 – 29) for a processing unit (see, e.g., FIG. 3, reference numerals 22 and 22'; page 11, line 5 – page 12, line 26). The processing unit is connectable to a data communications network (see, e.g., FIG. 1, reference numerals 2 and 3; page 10, lines 3 – 22). The portable storage device further includes an access controller (see, e.g., FIG. 4, reference numeral 59; FIG. 9, reference numeral 160; page 13, line 30 – page 14, line 2; page 20, lines 22 – 23) operable to prevent unauthorised writing to the storage (see, e.g., FIG. 9, reference numeral 160; page 20, lines 22 – 23; page 21, lines 7 – 14). The access controller is responsive to an unauthorised attempt to write to the storage to indicate that the write access has failed (see, e.g., FIG. 10, reference numerals 180, 184, and 186; page 22, lines 18 – 27; page 23, lines 4 – 10).

VI. GROUND S OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1, 4, 10, 13, 15, 20, 23, 25, 26, 29, and 30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien (PCT No. WO0857474) in view of Walters (U.S. Patent No. 5,357,573).
2. Claims 2, 11, and 21 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien in view of Walters and further in view of Braithwaite (U.S. Patent No. 5,644,444).
3. Claims 3, 12, 22, 27, and 28 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien in view of Walters and further in view of Hellman et al. (U.S. Patent No. 4,200,770), hereinafter "Hellman."

4. Claims 5, 14, 24, and 31 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien in view of Walters and further in view of “Windows NT Server.”

5. Claims 6, 7, and 16 – 18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien in view of Walters and further in view of Combaluzier (U.S. Patent No. 5,973,475).

6. Claim 8 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien in view of Walters and further in view of Teppler (U.S. Patent No. 6,792,536).

7. Claim 9 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien in view of Walters and further in view of Hastings et al. (U.S. Patent No. 5,460,411), hereinafter “Hastings.”

8. Claim 19 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien in view of Walters and Combaluzier and further in view of Teppler.

VII. ARGUMENT

First Ground of Rejection:

Claims 1, 4, 10, 13, 15, 20, 23, 25, 26, 29, and 30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien (PCT No. WO0857474) in view of Walters (U.S. Patent No. 5,357,573). Appellants traverse this rejection for the following reasons.

Claims 1, 4, 10, 13, 15, 20, 23, 25, 26, 29, and 30:

Merrien discloses a method and a system for using a smart card capable of being inserted in a terminal. Merrien further discloses storing in the card an Internet provider's

address, an IP address, and the card user's other personal Internet data; inserting the card in a card reader connected to the terminal; and activating an explorer to use the personal Internet data when the terminal is connected to the Internet.

Walters discloses a memory card (such as a PCMCIA card) which protects against unauthorized copying and use of software saved on the card. A read-only protection code is stored in the memory card. The protected software is supplemented by a protection routine which is activated upon execution of the software. The protection routine reads the protection code from the memory card and compares it to a comparison code contained within the protection routine. Use of the protected software will be allowed only if the two codes match.

In order to reject a claim as obvious, the Examiner has the burden of establishing a *prima facie* case of obviousness. *In re Warner et al.*, 379 F.2d 1011, 154 U.S.P.Q. 173, 177-178 (C.C.P.A. 1967). As stated in MPEP §2143 (Eighth Ed., Rev. 4), three basic criteria must be met to establish a *prima facie* case of obviousness: "First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations." With respect to claim 1, Appellants respectfully submit that the Examiner has not established a *prima facie* case for combining the cited references.

First, there is no suggestion or motivation to combine the references. The showing of a suggestion, teaching, or motivation to combine prior teachings "must be clear and particular Broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence'." *In re Dembiczak*, 175 F.3d 994, 50 USPQ2d 1614 (Fed. Cir. 1999). As held by the U.S. Court of Appeals for the Federal Circuit in *Ecolochem Inc. v. Southern California Edison Co.*, an obviousness claim that lacks evidence of a suggestion or motivation for one of skill in the art to combine prior art references to produce the claimed invention is defective as hindsight analysis. With

respect to claim 1, the Examiner argues that the motivation to combine Merrien and Walters is “to verify that the card input to the system was an approved card that could be used with the system.” The Examiner cites various locations in Walters (col. 2, lines 31 – 35; col. 2, line 60 to col. 3, line 3; col. 4, line 62 to col. 5, line 51) as including this motivation. However, there is no teaching either in the references cited or in the prior art to show how to combine the elements of Merrien with the elements of Walters to produce the claimed invention. Accordingly, Appellants submit that the obviousness rejection is defective as hindsight analysis.

Additionally, there is no reasonable expectation of success because the references cited by the Examiner teach away from each other. Merrien discloses a card which stores an IP address. The IP address openly and visibly identifies Merrien’s system on a computer network. By contrast, Walters discloses a card which stores a protection code. The code is strictly for internal use to ensure that copying or use of software is authorized. Making this code public, such as by using it as a network identity, would jeopardize the security of the code and thus undermine the security scheme disclosed by Walters.

Furthermore, Appellants respectfully submit that the cited references, singly or in combination, do not teach or suggest all the limitations of claim 1. In particular, the cited references do not teach or suggest “the processing unit being operable, before reading the network identity from the portable storage device, to attempt a write to the storage of the portable storage device, and, on determining that the write has failed, to read the supplied network identity.” The Final Office Action acknowledged that Merrien does not teach or suggest this limitation and instead cited Walters. At col. 5, lines 15 – 21, Walters discloses:

It is however possible to include a program routine in the BIOS of the specific PC which can read from the read-only memory device. This routine will initially attempt to write to this memory area. When this does not succeed the protection code will be read to guarantee that it is dealing with a functional protection code.

The protection code in Walters is intended only for internal use by the protection routine in the protected software. The protection code does not supply any information which is used outside of the authorization procedure. In particular, the protection code does not supply a network identity usable for access to a data communications network by a processing unit. The Final Office Action argued that the network identity comprises other data which can be read after the write-then-read technique of Walters is performed. However, Walters actually discloses a protection code which is usable to allow the execution of software associated with the particular protection code. There is no teaching or suggestion in Walters that verification of the protection code permits the reading of arbitrary data (i.e., data other than the executed software, such as the network identity of Merrien) from the card. Appellants therefore submit that the cited references, taken individually or in combination, do not teach or suggest “the processing unit being operable, before reading the network identity from the portable storage device, to attempt a write to the storage of the portable storage device, and, on determining that the write has failed, to read the supplied network identity” as recited in claim 1.

Accordingly, claim 1 and its dependent claim 4 are believed to patentably distinguish over the cited references for at least the reasons given above.

Claims 10, 20, and 25 recite features similar to those of claim 1 and are therefore believed to patentably distinguish over Merrien and Walters for at least the reasons given above. Dependent claims 13, 15, 23, 26, 29, and 30 are also believed to patentably distinguish over the art cited by the Final Office Action for similar reasons.

Second Ground of Rejection:

Claims 2, 11, and 21 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien in view of Walters and further in view of Braithwaite (U.S. Patent No. 5,644,444). Appellants traverse this rejection for the following reasons.

Claims 2, 11, and 21:

Claim 2 depends on claim 1 and is therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above. Claim 11 depends on claim 10 and is therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above. Claim 21 depends on claim 20 and is therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above.

Third Ground of Rejection:

Claims 3, 12, 22, 27, and 28 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien in view of Walters and further in view of Hellman et al. (U.S. Patent No. 4,200,770), hereinafter “Hellman.” Appellants traverse this rejection for the following reasons.

Claims 3, 12, 22, 27, and 28:

Claim 3 depends on claim 1 and is therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above. Claim 12 depends on claim 10 and is therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above. Claim 22 depends on claim 20 and is therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above. Claims 27 and 28 depend on claim 25 and are therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above.

Fourth Ground of Rejection:

Claims 5, 14, 24, and 31 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien in view of Walters and further in view of “Windows NT Server.” Appellants traverse this rejection for the following reasons.

Claims 5, 14, 24, and 31:

Claim 5 depends on claim 1 and is therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above. Claim 14 depends on claim 10 and is therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above. Claim 24 depends on claim 20 and is therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above. Claim 31 depends on claim 25 and is therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above.

Fifth Ground of Rejection:

Claims 6, 7, and 16 – 18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien in view of Walters and further in view of Combaluzier (U.S. Patent No. 5,973,475). Appellants traverse this rejection for the following reasons.

Claims 6, 7, and 16 – 18:

Claims 6 and 7 depend on claim 1 and are therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above. Claims 16 – 18 depend on claim 10 and are therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above.

Sixth Ground of Rejection:

Claim 8 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien in view of Walters and further in view of Teppler (U.S. Patent No. 6,792,536). Appellants traverse this rejection for the following reasons.

Claim 8 depends on claim 1 and is therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above.

Seventh Ground of Rejection:

Claim 9 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien in view of Walters and further in view of Hastings et al. (U.S. Patent No. 5,460,411), hereinafter “Hastings.” Appellants traverse this rejection for the following reasons.

Claim 9 depends on claim 1 and is therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above.

Eighth Ground of Rejection:

Claim 19 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Merrien in view of Walters and Combaluzier and further in view of Teppler. Appellants traverse this rejection for the following reasons.

Claim 19 depends on claim 10 and is therefore also believed to patentably distinguish over the art cited by the Final Office Action for the reasons given above.

For the foregoing reasons, it is submitted that the Examiner's rejection of claims 1 – 31 was erroneous, and reversal of the decision is respectfully requested.

The Commissioner is authorized to charge any fees that may be due to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 50-1505/5681-04100/BNK. This Appeal Brief is submitted with a return receipt postcard.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'B. Noël Kivlin', with a long horizontal flourish extending to the right.

B. Noël Kivlin
Reg. No. 33,929
ATTORNEY FOR APPELLANT(S)

Meyertons, Hood, Kivlin, Kowert and Goetzel, P.C.
P.O. Box 398
Austin, Texas 78767-0398
Phone: (512) 853-8800
Date: July 20, 2006

VIII. CLAIMS APPENDIX

The claims on appeal are as follows.

1. A processing unit connectable to a data communications network, the processing unit having a device reader for a portable storage device that includes storage operable to supply a network identity for the processing unit and an access controller, the access controller being operable to prevent unauthorised writing to the storage, the processing unit being operable, before reading the network identity from the portable storage device, to attempt a write to the storage of the portable storage device, and, on determining that the write has failed, to read the supplied network identity.
2. The processing unit of claim 1, wherein the processing unit is operable, on being powered up, to determine whether a said portable storage device is present in the device reader and, in the event that a said portable storage device is present in the device reader, to attempt a write to the storage of the portable storage device, the processing unit being further operable, on determining that the write has failed, to copy the supplied network identity from a data carrier to a second memory location and to use the supplied network identity.
3. The processing unit of claim 1, wherein access control logic of the portable storage device implements key-to-key encryption, the processing unit being operable to modify the content of the storage of the portable storage device by supplying a key to the access controller, and, in response to receipt of a return key from the access controller, to send an encrypted command to modify the content of the storage of the portable storage device.
4. The processing unit of claim 1, wherein the portable storage device is a smart card, the access controller is a microcontroller or a microprocessor, and the device reader is a smart card reader.

5. The processing unit of claim 1, wherein the network identity comprises a MAC address.
6. The processing unit of claim 1, comprising a service processor, the service processor being programmed to control reading of the portable storage device.
7. The processing unit of claim 6, wherein the service processor is a microcontroller.
8. The processing unit of claim 1, wherein the processing unit is a server computer.
9. The processing unit of claim 1, wherein the processing unit is a rack mountable computer server.
10. A control program for controlling the selection of a network identity for a processing unit connectable to a data communications network, the processing unit having a device reader for a portable storage device that includes storage operable to supply a network identity for the processing unit and an access controller, the access controller being operable to prevent unauthorised writing to the storage, the control program being operable, before reading the network identity from the portable storage device, to attempt a write to the storage of the portable storage device, and, only on determining that the write has failed, to read the supplied network identity.
11. The control program of claim 10, wherein the control program is operable, on the processing unit being powered up, to determine whether a said portable storage device is present in the device reader and, in the event that a said portable storage device is present in the device reader, to attempt a write to the storage of the portable storage device, the control program being further operable, on determining that the write has failed, to copy the supplied network identity from a data carrier to a second memory location and to use the supplied network identity.

12. The control program of claim 10, wherein access control logic of the portable storage device implements key-to-key encryption, the control program being operable to modify the content of the storage of the portable storage device by supplying a key to the access controller, and, in response to receipt of a return key from the access controller, to send an encrypted command to modify the content of the storage of the portable storage device.
13. The control program of claim 10, wherein the portable storage device is a smart card, the access controller is a microcontroller and the device reader is a smart card reader.
14. The control program of claim 10, wherein the network identity comprises a MAC address.
15. The control program of claim 10 on a carrier medium.
16. The control program of claim 10, wherein the processing unit comprises a service processor, the control program controlling operation of the service processor.
17. The control program of claim 16, wherein the service processor is a microcontroller.
18. A microcontroller comprising a control program as recited in claim 10.
19. A server computer comprising a device reader for reading a portable storage, a processor, memory and a microcontroller as recited in claim 18, the microcontroller being operable as a service processor and connected to read the content of storage in a portable storage device mounted in the portable storage device.

20. A method of controlling the selection of a network identity for a processing unit connectable to a data communications network, the processing unit comprising a device reader for a portable storage device that includes storage operable to supply a network identity for the processing unit and an access controller, the access controller being operable to prevent unauthorised writing to the storage, the method comprising:
attempting a write to the storage of the portable storage device; and
only on determining that the write has failed, reading the supplied network identity from the portable storage device.
21. The method of claim 20, further comprising:
on powering up of the processing unit, determining whether a said portable storage device is present in the device reader; and
in the event that a said portable storage device is present in the device reader,
attempting a write to the storage of the portable storage device, and
only on determining that the write has failed, copying the supplied network identity from a data carrier to a second memory location and using the supplied network identity.
22. The method of claim 20, wherein access control logic of the portable storage device implements key-to-key encryption, the method further comprising:
modifying the content of the storage of the portable storage device by supplying a key to the access controller; and
in response to receipt of a return key from the access controller, sending an encrypted command to modify the content of the storage of the portable storage device.
23. The method of claim 20, wherein the portable storage device is a smart card, the access controller is a microcontroller, and the device reader is a smart card reader.
24. The method of claim 20, wherein the network identity comprises a MAC address.

25. A portable storage device that includes storage containing a network identity for a processing unit connectable to a data communications network, the portable storage device further including an access controller operable to prevent unauthorised writing to the storage, access controller being responsive to an unauthorised attempt to write to the storage to indicate that the write access has failed.
26. The portable storage device of claims 25, further operable to respond to a read access to supply the network identity.
27. The portable storage device of claim 25, wherein the access controller implements key-to-key encryption, the access controller including key storage holding a stored key, the access controller being operable to compare a supplied key from the processing unit to the stored key and, in response to the supplied key verifying against the stored key, returning to the processing unit a return key derived from the stored key.
28. The portable storage device of claim 27, wherein the access controller is subsequently operable to respond to an encrypted command from the processing unit to modify the content of the storage in the portable storage device.
29. The portable storage device of claim 25, wherein the access controller is a microcontroller.
30. The portable storage device of claim 25, wherein the portable storage device is a smart card.
31. The portable storage unit of 25, wherein the network identity comprises a MAC address.

IX. EVIDENCE APPENDIX

No evidence submitted under 37 CFR §§ 1.130, 1.131, or 1.132 or otherwise entered by the Examiner is relied upon in this appeal.

X. RELATED PROCEEDINGS APPENDIX

There are no related proceedings known to Appellants, Appellants' legal representatives, or assignee which will directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.